Variant Narrowing and Equational Unification

Santiago Escobar[1], José Meseguer[2] and Ralf Sasse[2]

[1] Universidad Politécnica de Valencia, Spain. sescobar@dsic.upv.es
[2] University of Illinois at Urbana-Champaign, USA.
{meseguer,rsasse}@cs.uiuc.edu

Abstract. Narrowing is a well-known complete procedure for equational E-unification when E can be decomposed as a union $E = \Delta \uplus B$ with B a set of axioms for which a finitary unification algorithm exists, and Δ a set of confluent, terminating, and B-coherent rewrite rules. However, when $B \neq \emptyset$, efficient narrowing strategies such as basic narrowing easily fail to be complete and cannot be used. This poses two challenges to narrowing-based equational unification: (i) finding efficient narrowing strategies that are complete modulo B under mild assumptions on B, and (ii) finding sufficient conditions under which such narrowing strategies yield *finitary* E-unification algorithms. Inspired by Comon and Delaune's notion of E-variant for a term, we propose a new narrowing strategy called *variant narrowing* that has a search space potentially much smaller than full narrowing, is complete, and yields a finitary E-unification algorithm when E has the finite variant property. We furthermore identify a class of equational theories for which the finite bound ensuring the finite variant property can be effectively computed by a generic algorithm. We also discuss applications to the formal analysis of cryptographic protocols modulo the algebraic properties of the underlying cryptographic functions.

1 Introduction

Equational unification is the solving of existentially quantified problems $\exists \boldsymbol{x}\ t =_E t'$ modulo an equational theory E. If the equations E are convergent, it is well-known that narrowing provides a complete unification procedure for E-unification [8]. This result extends to narrowing modulo a set B of equational axioms. That is, if $E = \Delta \uplus B$, where Δ is a set of oriented equations that are convergent and coherent modulo B, then narrowing with Δ modulo B is also a complete E-unification procedure [9]. In practice, however, full narrowing, i.e., considering all narrowing sequences, can be highly inefficient. This has led to the search for complete narrowing strategies that have a much smaller search space; and to conditions under which narrowing terminates, so that a finitary unification algorithm can be obtained. Hullot's basic narrowing [8] is one such strategy, which is complete, uses only normalized unifiers, and terminates under suitable conditions. The problem, however, is that basic narrowing is complete for $B = \emptyset$, but is *incomplete* for a general set B of axioms, and in particular for associativity-commutativity (AC) (see [16,1] and Example 14).

This paper addresses the problem of finding complete narrowing procedures modulo B, under minimal assumptions on B, which have a much smaller search space than full narrowing, and for which termination conditions can be given. Specifically, inspired by the notion of E-variant of a term due to Comon and Delaune [1], we propose a new narrowing method called *variant narrowing* with the following properties: (i) it only uses substitutions in normal form modulo B; (ii) it is complete under very general assumptions on B and Δ; (ii) if Δ has the finite variant property modulo B, it can be used to both compute all the finite variants of a term in a very space-efficient way, and to obtain a *finitary* E-unification algorithm.

Regarding termination conditions, we show that for equational theories that are *strongly right irreducible* and *innermost preserving* the following properties hold: (i) a bound can effectively be computed ensuring the finite variant property; (ii) variant narrowing can then be specialized to two algorithms, one for computing the finite set of variants of any term, and another providing a finitary E-unification algorithm.

Our own, specific motivation for working on this topic comes from our work on narrowing-based formal analysis of cryptographic protocols *modulo* equational assumptions about the cryptographic functions and on tools supporting such kind of analysis [4,5,3]. Even assuming that an underlying implementation supports unification modulo a family of different equational axiom theories $B_1, \ldots B_n$ as well as their modular combinations (as for example the current Maude implementation that we use does), there are many cryptographic theories E for which a finitary unification algorithm is not readily available. However, as shown by Comon and Delaune in [1], various cryptographic theories enjoy the finite variant property. Our proposed variant narrowing procedure then provides an efficient (from the state space size point of view) way of computing a complete and minimal finite set of E-unifiers for the cryptographic theory E, which is decomposed as a pair $E = \Delta \uplus B$, with Δ confluent, terminating, and coherent modulo B, and B a modular combination of the axioms $B_1, \ldots B_n$ supported in a built-in way by the underlying implementation. Our own experience (see [5,3]) has taught us an important additional lesson, namely, that a typed setting supporting sorts and subsorts can greatly help in making narrowing-based unification algorithms terminating. For this reason, we develop the entire paper in the setting of order-sorted equational theories.

The paper is organized as follows. In Section 2 we explain basic concepts and rewriting. Then in Section 3 we introduce the necessary narrowing concepts. In Section 4 we recap results about variants and explains our variant narrowing approach. Section 5 describes our variant narrowing procedure for equational unification, and we conclude in Section 6 and discuss related and future work.

2 Preliminaries

We follow the classical notation and terminology from [15] for term rewriting and from [11,12] for rewriting logic and order-sorted notions. We assume an

order-sorted signature Σ with a finite poset of sorts $(\mathsf{S}, \leq)$ and a finite number of function symbols. We furthermore assume that: (i) each connected component in the poset ordering has a top sort, and for each $\mathsf{s} \in \mathsf{S}$ we denote by $[\mathsf{s}]$ the top sort in the component of s; and (ii) for each operator declaration $f : \mathsf{s}_1 \times \ldots \times \mathsf{s}_n \to \mathsf{s}$ in Σ, there is also a declaration $f : [\mathsf{s}_1] \times \ldots \times [\mathsf{s}_n] \to [\mathsf{s}]$. We assume an S-sorted family $\mathcal{X} = \{\mathcal{X}_\mathsf{s}\}_{\mathsf{s} \in \mathsf{S}}$ of disjoint variable sets with each $\mathcal{X}_\mathsf{s}$ countably infinite. $\mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ is the set of terms of sort s, and $\mathcal{T}_{\Sigma,\mathsf{s}}$ is the set of ground terms of sort s. We write $\mathcal{T}_\Sigma(\mathcal{X})$ and $\mathcal{T}_\Sigma$ for the corresponding term algebras. For a term t we write $Var(t)$ for the set of all variables in t. The set of positions of a term t is written $Pos(t)$, and the set of non-variable positions $Pos_\Sigma(t)$. The root of a term is Λ. The subterm of t at position p is $t|_p$ and $t[u]_p$ is the subterm $t|_p$ in t replaced by u. A *substitution* σ is a sorted mapping from a finite subset of $\mathcal{X}$, written $Dom(\sigma)$, to $\mathcal{T}_\Sigma(\mathcal{X})$. The set of variables introduced by σ is $Ran(\sigma)$. The identity substitution is *id*. Substitutions are homomorphically extended to $\mathcal{T}_\Sigma(\mathcal{X})$. The application of a substitution σ to a term t is denoted by $t\sigma$. The restriction of σ to a set of variables V is $\sigma|_V$. Composition of two substitutions is denoted by $\sigma\sigma'$, meaning $\sigma\sigma'(X) = (X\sigma)\sigma'$ for any variable X. We call a substitution σ a *renaming* if there is another substitution σ^{-1} such that $\sigma\sigma^{-1} = id$.

A Σ*-equation* is an unoriented pair $t = t'$, where $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. Given Σ and a set E of Σ-equations such that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s, order-sorted equational logic induces a congruence relation $=_E$ on terms $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$ (see [12]). Throughout this paper we assume that $\mathcal{T}_{\Sigma,\mathsf{s}} \neq \emptyset$ for every sort s. An *equational theory* (Σ, E) is a set of Σ-equations.

The E*-subsumption* preorder $\leq_E$ (or $\leq$ if E is understood) holds between $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$, denoted $t \leq_E t'$ (meaning that t is more general than t'), if there is a substitution σ such that $t\sigma =_E t'$; such a substitution σ is said to be an E*-match* from t to t'. For substitutions σ, ρ and a set of variables V we define $\sigma|_V =_E \rho|_V$ if $x\sigma =_E x\rho$ for all $x \in V$; $\sigma|_V \leq_E \rho|_V$ if there is a substitution η such that $(\sigma\eta)|_V =_E \rho|_V$; and $\sigma|_V \simeq_E \rho|_V$ if there is a renaming η such that $(\sigma\eta)|_V =_E \rho|_V$.

An E*-unifier* for a Σ-equation $t = t'$ is a substitution σ such that $t\sigma =_E t'\sigma$. For $Var(t) \cup Var(t') \subseteq W$, a set of substitutions $CSU_E(t = t')$ is said to be a *complete* set of unifiers of the equation $t =_E t'$ away from W if: (i) each $\sigma \in CSU_E(t = t')$ is an E-unifier of $t =_E t'$; (ii) for any E-unifier ρ of $t =_E t'$ there is a $\sigma \in CSU_E(t = t')$ such that $\sigma|_V \leq_E \rho|_V$ and $V = Var(t) \cup Var(t')$; (iii) for all $\sigma \in CSU_E(t = t')$, $Dom(\sigma) \subseteq (Var(t) \cup Var(t'))$ and $Ran(\sigma) \cap W = \emptyset$. An E-unification algorithm is *complete* if for any equation $t = t'$ it generates a complete set of E-unifiers. Note that this set needs not be finite. A unification algorithm is said to be *finitary* and complete if it always terminates after generating a finite and complete set of solutions. A unification algorithm is said to be *minimal* if it always provides a minimal set of unifiers.

A *rewrite rule* is an oriented pair $l \to r$, where $l \notin \mathcal{X}$, and $l, r \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ for some sort $\mathsf{s} \in \mathsf{S}$. An *(unconditional) order-sorted rewrite theory* is a triple $\mathcal{R} = (\Sigma, E, R)$ with Σ an order-sorted signature, E a set of Σ-equations, and R a set of rewrite rules. The rewriting relation on $\mathcal{T}_\Sigma(\mathcal{X})$, written $t \to_R t'$ or

$t \xrightarrow{p}_R t'$ holds between t and t' iff there exist $p \in Pos_\Sigma(t)$, $l \to r \in R$ and a substitution σ, such that $t|_p = l\sigma$, and $t' = t[r\sigma]_p$. The relation $\to_{R/E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ is $=_E;\to_R;=_E$. Note that $\to_{R/E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ induces a relation $\to_{R/E}$ on $\mathcal{T}_{\Sigma/E}(\mathcal{X})$ by $[t]_E \to_{R/E} [t']_E$ iff $t \to_{R/E} t'$. The transitive closure of $\to_{R/E}$ is denoted by $\to^+_{R/E}$ and the transitive and symmetric closure of $\to_{R/E}$ is denoted by $\to^*_{R/E}$. We say that a term t is $\to_{R/E}$-irreducible (or just R/E-irreducible) if there is no term t' such that $t \to_{R/E} t'$.

We say that the relation $\to_{R/E}$ is *terminating* if there is no infinite sequence $t_1 \to_{R/E} t_2 \to_{R/E} \cdots \to_{R/E} \cdots$. We say that the relation $\to_{R/E}$ is *confluent* if, given terms $t, t', t'' \in \mathcal{T}_\Sigma(\mathcal{X})$, whenever $t \to^*_{R/E} t'$ and $t \to^*_{R/E} t''$, there exists a term t''' such that $t' \to^*_{R/E} t'''$ and $t'' \to^*_{R/E} t'''$. We say that $\to_{R/E}$ is *convergent* if it is confluent and terminating. An order-sorted rewrite theory $\mathcal{R} = (\Sigma, E, R)$ is convergent (resp. terminating, confluent) if the relation $\to_{R/E}$ is convergent (resp. terminating, confluent). In a convergent order-sorted rewrite theory, for each term $t \in \mathcal{T}_\Sigma(\mathcal{X})$, there is a unique (up to E-equivalence) R/E-irreducible term t' obtained from t by rewriting to canonical form, which is denoted by $t \to^!_{R/E} t'$ or $t{\downarrow_{R/E}}$ (when t' is not relevant).

For substitutions σ, ρ and a set of variables V we define $\sigma|_V \to_{R/E} \rho|_V$ if there is $X \in V$ such that $X\sigma \to_{R/E} X\rho$ and for all other $Y \in V$ we have $Y\sigma =_E Y\rho$. A substitution σ is called *R/E-normalized* if $X\sigma$ is R/E-irreducible for all X.

2.1 R, E-rewriting

Since E-congruence classes can be infinite, $\to_{R/E}$-reducibility is undecidable in general. Therefore, R/E-rewriting is usually implemented [9] by R, E-rewriting. We assume the following properties on R and E:

1. E is *regular*, i.e., for each $t = t'$ in E, we have $Var(t) = Var(t')$, and *sort-preserving*, i.e., for each substitution σ, we have $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ if and only if $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$, and all variables in $Var(t)$ have a top sort.
2. E has a finitary and complete unification algorithm, which implies that E-matching is finitary and complete.
3. For each $t \to t'$ in R we have $Var(t') \subseteq Var(t)$.
4. R is *sort-decreasing*, i.e., for each $t \to t'$ in R, each $\mathsf{s} \in \mathsf{S}$, and each substitution σ, $t'\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$ implies $t\sigma \in \mathcal{T}_\Sigma(\mathcal{X})_\mathsf{s}$.
5. The rewrite rules R are *confluent and terminating modulo* E, i.e., the relation $\to_{R/E}$ is confluent and terminating.

Definition 1 (R, E-rewriting). [17] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(5) *above. We define the relation $\to_{R,E}$ on $\mathcal{T}_\Sigma(\mathcal{X})$ by $t \to_{R,E} t'$ iff there is a $p \in Pos_\Sigma(t)$, $l \to r$ in R and substitution σ such that $t|_p =_E l\sigma$ and $t' = t[r\sigma]_p$.*

Note that, since E-matching is decidable, $\to_{R,E}$ is decidable. Notions such as confluence, termination, irreducible terms or normalized substitution are defined

in a straightforward manner for $\rightarrow_{R,E}$. Note that since R is convergent (modulo E), the relation $\rightarrow^{!}_{R,E}$ is decidable, i.e., it terminates and produces a unique term (up to E-equivalence) for each initial term. Of course $t \rightarrow_{R,E} t'$ implies $t \rightarrow_{R/E} t'$, but the converse need not hold. To prove completeness of $\rightarrow_{R,E}$ w.r.t. $\rightarrow_{R/E}$ we need the following additional assumption.

6. $\rightarrow_{R,E}$ is *E-coherent* [9], i.e., $\forall t_1, t_2, t_3$ we have $t_1 \rightarrow_{R,E} t_2$ and $t_1 =_E t_3$ implies $\exists t_4, t_5$ such that $t_2 \rightarrow^{*}_{R,E} t_4$, $t_3 \rightarrow^{+}_{R,E} t_5$, and $t_4 =_E t_5$.

The following theorem originally established in [9, Proposition 1] and extended to order-sorted theories links $\rightarrow_{R/E}$ with $\rightarrow_{R,E}$.

Theorem 1 (Correspondence). [9] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *above. Then $t_1 \rightarrow^{!}_{R/E} t_2$ if and only if $t_1 \rightarrow^{!}_{R,E} t_2$.*

3 *R, E*-Narrowing

Narrowing generalizes rewriting by performing unification at non-variable positions instead of the usual matching. The essential idea behind narrowing is to *symbolically* represent the rewriting relation between terms as a narrowing relation between more general terms.

Definition 2 (R, E-narrowing). *(see, e.g.,* [9,13]*) Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *above. The R, E-narrowing relation on $\mathcal{T}_{\Sigma}(\mathcal{X})$ is defined as $t \overset{\sigma}{\rightsquigarrow}_{R,E} t'$ (or $\overset{\sigma}{\rightsquigarrow}$ if R, E is understood) if there is $p \in Pos_{\Sigma}(t)$, a rule $l \rightarrow r$ in R (where we always assume $Var(t) \cap (Var(l) \cup Var(r)) = \emptyset$), and $\sigma \in CSU_E(t|_p = l)$ such that $t' = (t[r]_p)\sigma$.*

The following results originally established in [9, Propositions 2 and 3] and extended to order-sorted theories link $\rightarrow_{R,E}$ with $\rightsquigarrow_{R,E}$.

Theorem 2 (Correctness). [9] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *above. If $t_1 \overset{\theta}{\rightsquigarrow}^{*}_{R,E} t_2$, then for any substitution ρ, $t_1\theta\rho \rightarrow^{*}_{R,E} t_2\rho$. Furthermore, the number of narrowing steps in $t_1 \overset{\theta}{\rightsquigarrow}^{*}_{R,E} t_2$ coincides with the number of rewrite steps in $t_1\theta\rho \rightarrow^{*}_{R,E} t_2\rho$.*

Theorem 3 (Completeness w.r.t. normalized substitutions). [9] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *above. Let t_1 be a term and θ a R, E-normalized substitution. If $t_1\theta \rightarrow^{!}_{R,E} t_2$, then there exists a term t'_2 and two R, E-normalized substitutions θ' and ρ s.t. $t_1 \overset{\theta'}{\rightsquigarrow}^{*}_{R,E} t'_2$, $\theta|_{Var(t_1)} =_E (\theta'\rho)|_{Var(t_1)}$, and $t_2 =_E t'_2\rho$. Furthermore, the number of rewriting and narrowing steps coincide.*

We can easily extend the previous result to allow non-normalized substitutions.

Lemma 1 (Completeness). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *above. Let t_1 be a term and θ be any substitution. If $t_1\theta \to^!_{R,E} t_2$, then there exists a term t_2' and two R,E-normalized substitutions θ' and ρ s.t. $t_1 \overset{\theta'}{\leadsto}{}^*_{R,E} t_2'$, $\theta{\downarrow_{R,E}}|_{Var(t_1)} =_E (\theta'\rho)|_{Var(t_1)}$, and $t_2 =_E t_2'\rho$.*

Proof. By confluence and termination of $\to_{R,E}$, $t_1\theta \to^!_{R,E} t_2$ implies $t_1\theta' \to^!_{R,E} t_2$ for $\theta' = \theta{\downarrow_{R,E}}$ and, by Theorem 3, there exists a term t_2' and two R,E-normalized substitutions σ and ρ s.t. $t_1 \overset{\sigma}{\leadsto}{}^*_{R,E} t_2'$, $\theta'|_{Var(t_1)} =_E (\sigma\rho)|_{Var(t_1)}$, and $t_2 =_E t_2'\rho$. □

The narrowing relation $\leadsto_{R,E}$ is known to give a sound and complete $R \uplus E$-unification procedure [9, Theorem 5] that under assumptions (1)–(6) can be extended to order-sorted theories in a straightforward way. By abuse of notation, we view $R \uplus E$ as an equational theory even though R is defined as a set of rules instead of a set of equations.

Theorem 4 (Complete $R \uplus E$-unification procedure). [9] *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *above. Let t, t' be two terms. Then, $\sigma \in CSU_{R\uplus E}(t = t')$ if and only if $(t \approx t') \overset{\sigma}{\leadsto}{}^*_{\widehat{R},E} \mathtt{tt}$, where $\approx$ and $\mathtt{tt}$ are new symbols* [3] *and $\widehat{R} = R \cup \{x \approx x \to \mathtt{tt}\}$. The set $CSU_{R\uplus E}(t = t')$ of unifiers is* finitary *if $CSU_{R\uplus E}(t = t')$ can always be generated from a finite number of finite narrowing sequences $(t \approx t') \overset{\theta}{\leadsto}{}^*_{\widehat{R},E} \mathtt{tt}$.*

When we restrict ourselves to order-sorted rewrite theories satisfying properties (1)–(6) above, the complete set of unifiers of two terms can be restricted to normalized substitutions without loss of generality, as shown in the following Proposition. Moreover, we can obtain a minimal complete set of unifiers by considering only the most general normalized substitutions.

Proposition 1 (Completeness under most general normalized substitutions). *Let $\mathcal{R} = (\Sigma, E, R)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *above. Let t, t' be two terms. If $\sigma \in CSU_{R\uplus E}(t = t')$, then there exist substitutions θ and ρ s.t. $\theta \in CSU_{R\uplus E}(t = t')$ and $\sigma{\downarrow_{R,E}} =_E \theta\rho$.*

Proof. By Lemma 1. □

4 Variants and Variant Narrowing

Although the narrowing relation $\leadsto_{R,E}$ gives a sound and complete $R \uplus E$-unification procedure, narrowing can be infinite in general, that is, this $R \uplus E$-unification procedure may not be finitary. A natural approach would be to study classes of rewrite theories where the narrowing relation $\leadsto_{R,E}$ is terminating, as

[3] That is, we extend Σ to $\widehat{\Sigma}$ by adding a new sort Truth, not related to any sort in Σ, with constant $\mathtt{tt}$, and for each top sort of a connected component [s], an operator $\approx$: [s] × [s] → Truth.

for the case when $E = \emptyset$ studied in [8,10,2,14]. However, narrowing modulo E can generate many infinite sequences, specially when we consider associativity and commutativity axioms, as shown in [1,16], making it impossible to extend the good termination properties of previously studied classes of rewrite theories. In this paper, we propose a new notion of narrowing modulo axioms B, called *variant narrowing*, that (i) is complete for any set B of axioms satisfying the properties (1)–(6) and avoids many wasteful narrowing sequences that would be created by full narrowing; and (ii) if the rules R satisfy the finite variant property modulo B as defined by Comon and Delaune, [1], then can be specialized into a *terminating* complete narrowing algorithm. We first need the notion of decomposition of an equational theory into rules and axioms.

Definition 3 (Decomposition). *Let (Σ, E) be an order-sorted equational theory. We call (Δ, B) a* decomposition *of E if (Σ, B, Δ) is an order-sorted rewrite theory satisfying properties* (1)–(6).

Example 1. Let us consider the following equational theory for the exclusive or operator and the cancellation equations for public encryption/decryption. The exclusive or symbol $\oplus$ has associative and commutative (AC) properties with 0 as its unit. The symbol pk is used for public key encryption and the symbol sk for private key encryption. The equations E are as follows.

$$X \oplus 0 = X \tag{1}$$
$$X \oplus X = 0 \tag{2}$$
$$X \oplus X \oplus Y = Y \tag{3}$$
$$pk(K, sk(K, M)) = M \tag{4}$$
$$sk(K, pk(K, M)) = M \tag{5}$$
$$X \oplus (Y \oplus Z) = (X \oplus Y) \oplus Z \tag{6}$$
$$X \oplus Y = Y \oplus X \tag{7}$$

This equational theory (Σ, E) has a decomposition into Δ containing the oriented version of equations (1)–(5) and B containing the last two associativity and commutativity equations (6)–(7) for $\oplus$. Note that Equation (3) is necessary to obtain AC-coherence of the rules (1)–(5).

Since narrowing can be infinite in general (specially when we consider associativity and commutativity axioms) we use the notion of *finite variants* and the *finite variant property* proposed by Comon and Delaune in [1] as a technical concept that will provide a suitable characterization of unification w.r.t. an equational theory E in terms of narrowing.

Definition 4 (Variants). [1] *Given a term t and an equational theory E, we say that (t', θ) is an* E-variant *of t if $t\theta =_E t'$.*

Definition 5 (Complete set of variants). [1] *Let (Δ, B) be a decomposition of an equational theory (Σ, E). A* complete set of E-variants *of a term t, denoted*

$FV_{\Delta,B}(t)$, is a set S of E-variants of t such that, for each substitution σ, there is a variant $(t', \rho) \in S$ and a substitutions θ such that: (i) $(t\sigma)\downarrow_{\Delta,B} =_B t'\theta$, and (ii) $(\sigma\downarrow_{\Delta,B})|_{Var(t)} =_B (\rho\theta)|_{Var(t)}$.

Note that, by the previous definition, any pair $(t', \rho) \in FV_{\Delta,B}(t)$ satisfies that t' is Δ, B-irreducible and ρ is Δ, B-normalized.

Definition 6 (Finite variant property). [1] *Let (Δ, B) be a decomposition of an order-sorted equational theory (Σ, E). Then E, and thus (Δ, B), have the* finite variant property *if for each term t, we can compute a finite complete set of E-variants. We will call (Δ, B) a* finite variant decomposition *if (Δ, B) has the finite variant property.*

Example 2. For (Σ, E) the theory in Example 1, the term $t = M \oplus sk(K, pk(K, M))$ has $(0, id)$ as an E-variant. In fact, $(0, id)$ is a *complete* set of E-variants, because for any substitution σ we have $t\sigma\downarrow_{\Delta,B} = 0 =_B 0id$. Thus this one variant fulfills the requirements of being a complete set of E-variants of t.

For the term $s = X \oplus sk(K, pk(K, Y))$ we get two variants that make up the complete set of E-variants. First, we have (s', θ) with $s' = 0$ and $\theta = \{X/Y\}$ as one E-variant, and (s'', id) with $s'' = X \oplus Y$ as the other variant. Thus, $S = \{(s', \theta), (s'', id)\}$ is a complete set of E-variants for s, since whenever the substitution σ is such that $X\sigma\downarrow_{\Delta,B} = Y\sigma\downarrow_{\Delta,B}$, then $s\sigma\downarrow_{\Delta,B} = 0 =_B s'id$; and whenever σ is such that $X\sigma\downarrow_{\Delta,B} \neq Y\sigma\downarrow_{\Delta,B}$ then $s\sigma\downarrow_{\Delta,B} = X\sigma\downarrow_{\Delta,B} \oplus Y\sigma\downarrow_{\Delta,B} =_B s''\theta$ where $\theta =_B \sigma\downarrow_{\Delta,B}$.

The following result from Comon and Delaune provides the necessary connection between a decomposition and the finite variant property.

Lemma 2. [1] *Let (Δ, B) be a decomposition of an equational theory (Σ, E). (Δ, B) satisfies the finite variant property if and only if for every term t, there is a finite set $\Theta(t)$ of substitutions such that*

$$\forall\sigma, \exists\theta \in \Theta(t), \exists\tau \text{ s.t. } (\sigma\downarrow_{\Delta,B})|_{Var(t)} =_B (\theta\tau)|_{Var(t)} \wedge (t\sigma)\downarrow_{\Delta,B} =_B ((t\theta)\downarrow_{\Delta,B})\tau$$

Informally, if there is a finite number of substitutions, satisfying the properties of Lemma 2, then narrowing should be able to find those substitutions after a finite number of steps. This idea is characterized by the following definition.

Definition 7 (Boundedness property). [1] *Let (Δ, B) be a decomposition of an equational theory (Σ, E). (Δ, B) satisfies the* boundedness property *if for every term t there exists an integer n, denoted by $\#_{\Delta,B}(t)$, such that for every Δ, B-normalized substitution σ the normal form of $t\sigma$ is reachable by a Δ, B-rewriting derivation whose length can be bounded by n (thus independently of σ):*

$$\forall t, \exists n, \forall\sigma. t(\sigma\downarrow_{\Delta,B}) \xrightarrow{\leq n}_{\Delta,B} (t\sigma)\downarrow_{\Delta,B}$$

Finally, the following result provides the necessary connection between the boundedness property and the finite variant property.

Theorem 5. [1] *Let (Δ, B) be a decomposition of an equational theory (Σ, E). Then, (Δ, B) satisfies the boundedness property if and only if (Δ, B) is a finite variant decomposition of (Σ, E).*

We can compute a complete set $FV_{\Delta,B}(t)$ of finite variants of a term t using the narrowing relation $\rightsquigarrow_{\Delta,B}$. If we would take the variants to be those $\rightarrow_{\Delta,B}$-irreducible terms found at the leaves of the narrowing sequences generated by $\rightsquigarrow^*_{\Delta,B}$, i.e., $(s,\sigma) \in FV_{\Delta,B}(t)$ if and only if there is a narrowing derivation $t \overset{\sigma'}{\rightsquigarrow}{}^{n}_{\Delta,B} s$ such that $\sigma \simeq_B \sigma'$, s is $\rightarrow_{\Delta,B}$-irreducible, σ is $\rightarrow_{\Delta,B}$-normalized, and either $n = \#_{\Delta,B}(t)$ (in the limit) or there is no s' such that $s \rightsquigarrow_{\Delta,B} s'$ (a leaf), then we would be able to decide E-unification based on that. But, for a *complete* set of variants we need the intermediate terms. This is shown by the following example.

Example 3. If we restrict ourselves to use only leaves of the narrowing sequence as variants, and look at term $s = X \oplus sk(K, pk(K,Y))$ in Example 4, then even though $s \overset{id}{\rightsquigarrow}{}^*_{\Delta,B} X \oplus Y$ we cannot say that $(X \oplus Y, id)$ is a variant, because we have the following further narrowing step $X \oplus Y \overset{X/Y}{\rightsquigarrow}{}^*_{\Delta,B} 0$. But, then $(0, X/Y)$ is not a complete set of variants of s anymore. This can be seen by considering $\sigma = id$, then $s\sigma{\downarrow_\Delta} = X \oplus Y$ but there is no substitution θ so that $X \oplus Y =_B 0\theta$.

Therefore, we effectively compute a complete set of variants in the following form.

Proposition 2 (Computing the Finite Variants I). *Let (Δ, B) be a finite variant decomposition of an order-sorted equational theory (Σ, E). Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\#_{\Delta,B}(t) = n$. Then $(s,\sigma) \in FV_{\Delta,B}(t)$ if and only if there is a narrowing derivation $t \overset{\sigma'}{\rightsquigarrow}{}^{\leq n}_{\Delta,B} s$ such that $\sigma \simeq_B \sigma'$, s is $\rightarrow_{\Delta,B}$-irreducible and σ is $\rightarrow_{\Delta,B}$-normalized.*

Proof. Note that because of boundedness of rewriting sequences and Theorem 3 we get a finite set (up to renaming) of finite narrowing sequences that is enough to obtain all variants of t. Then we consider the two directions of the equivalence:

($\Rightarrow$) $(s,\sigma) \in FV_{\Delta,B}(t)$ means that $t\sigma \rightarrow^!_{\Delta,B} s$, and σ is normalized. Thus, by Theorem 3, $t \overset{\sigma}{\rightsquigarrow}{}^*_{\Delta,B} s$.

($\Leftarrow$) $t \overset{\sigma}{\rightsquigarrow}{}^*_{\Delta,B} s$ when s is $\rightarrow_{\Delta,B}$-irreducible and σ is $\rightarrow_{\Delta,B}$-normalized implies $(s,\sigma) \in FV_{\Delta,B}(t)$. □

Example 4. Our theory from Example 1 has the boundedness property, as we will see below in Example 6. Thus, we can use Proposition 2 to get E-variants of $t = M \oplus sk(K, pk(K,M))$. As $t \rightarrow^!_{\Delta,B} 0$ we have $t \overset{id}{\rightsquigarrow}{}^!_{\Delta,B} 0$. Therefore, $(0, id) \in FV_{\Delta,B}(t)$ and it is the only element of the complete set of E-variants as no other narrowing sequences are possible.

For $s = X \oplus sk(K, pk(K,Y))$ we get $s \overset{id}{\rightsquigarrow}{}^*_{\Delta,B} X \oplus Y$ and $s \overset{X/Y}{\rightsquigarrow}{}^*_{\Delta,B} 0$ so $(X \oplus Y, id)$ and $(0, X/Y)$ are the variants. As no other narrowing sequences are possible these two make up a complete set of E-variants.

4.1 Variant Narrowing

Let us first motivate why an alternative narrowing strategy is necessary for confluent and terminating rewrite theories modulo axioms B. Applying narrowing $\rightsquigarrow_{\Delta,B}$ to perform $(\Delta \uplus B)$-unification without any restrictions is very wasteful, because as soon as a rewrite step $\rightarrow_{\Delta,B}$ is enabled in a term that has also narrowing steps $\rightsquigarrow_{\Delta,B}$, that rewrite step should be taken before any further narrowing steps are applied, thanks to confluence modulo B. This idea is consistent with the implementation of rewriting logic [17] and, therefore, the relation $\rightarrow^{!}_{\Delta,B}; \rightsquigarrow_{\Delta,B}$ makes sense as an optimization of $\rightsquigarrow_{\Delta,B}$. However, this is still a naive approach, since a rewrite step and a narrowing step satisfy a more general property which is the reason for being able to take the rewrite step and avoiding the narrowing step. Namely, if two narrowing steps $t \overset{\sigma_1}{\rightsquigarrow}_{\Delta,B} t_1$ and $t \overset{\sigma_2}{\rightsquigarrow}_{\Delta,B} t_2$ are possible and we have that $\sigma_1 \leq_B \sigma_2$ (i.e., σ_1 is more general than σ_2), then it is enough to take only the narrowing step using σ_1. These improvements are formalized as follows.

Definition 8 (Preorder and equivalence of narrowing steps). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. Let us consider two narrowing steps $\alpha_1 : t \overset{\sigma_1}{\rightsquigarrow}_{\Delta,B} s_1$ and $\alpha_2 : t \overset{\sigma_2}{\rightsquigarrow}_{\Delta,B} s_2$. We write $\alpha_1 \preceq_B \alpha_2$ if $\sigma_1 \leq_B \sigma_2$ and $\alpha_1 \prec_B \alpha_2$ if $\sigma_1 <_B \sigma_2$ (i.e., σ_1 is strictly more general than σ_2). The relation $\alpha_1 \preceq_B \alpha_2 \wedge \alpha_2 \preceq_B \alpha_1$ between two narrowing steps from t defines a set of equivalence classes between such narrowing steps, which we denote by $\alpha_1 \simeq_B \alpha_2$. In what follows we will be interested in choosing a unique representation $\underline{\alpha} \in [\alpha]_{\simeq_B}$ in each equivalence class of narrowing steps from t. Therefore, $\underline{\alpha}$ will always denote a chosen unique representative $\underline{\alpha} \in [\alpha]_{\simeq_B}$.*

Definition 9 (Variant Narrowing). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. We define $t \overset{p,\sigma}{\rightsquigarrow}_{\underline{\Delta},B} s$ as $\underline{\alpha} : t \overset{p,\sigma}{\rightsquigarrow}_{\Delta,B} s$ such that σ is normalized, $\underline{\alpha}$ is minimal w.r.t. the order $\preceq_B$, and $\underline{\alpha}$ is a chosen unique representative of its $\simeq_B$-equivalence class.*

Note that the relation $\rightarrow^{!}_{\Delta,B}; \rightsquigarrow_{\Delta,B}$ is (appropriately) simulated by $\rightsquigarrow_{\underline{\Delta},B}$, since in $\rightsquigarrow_{\underline{\Delta},B}$ rewriting steps are always given priority over narrowing steps.

Lemma 3 (Normalization of Variant Narrowing). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. Let $t \in \mathcal{T}_{\Sigma}(\mathcal{X})$. If t is not Δ, B-irreducible, then there is a unique $\rightsquigarrow_{\underline{\Delta},B}$-narrowing sequence from t such that $t \overset{id}{\rightsquigarrow}^{*}_{\underline{\Delta},B} t{\downarrow_{\Delta,B}}$.*

Proof. Immediate by Definition 9, since rewriting steps have the most general substitutions and one rewriting step is chosen among all the available ones by each step in $\rightsquigarrow^{*}_{\underline{\Delta},B}$. □

The following result ensures that variant narrowing is complete.

Theorem 6 (Completeness of Variant Narrowing). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. If $t \overset{\sigma}{\rightsquigarrow}^{*}_{\Delta,B} t\sigma{\downarrow_{\Delta,B}}$*

with σ Δ, B-normalized, and there are no substitutions ρ, ρ' such that $t \overset{\rho}{\leadsto}{}^*_{\Delta,B} t\rho{\downarrow}_{\Delta,B}$, $t\sigma{\downarrow}_{\Delta,B} =_B (t\rho{\downarrow}_{\Delta,B})\rho'$, $\sigma|_{Var(t)} =_B (\rho\rho')|_{Var(t)}$, and $\rho' \neq id$, then $t \overset{\sigma}{\leadsto}{}^*_{\underline{\Delta},B} t\sigma{\downarrow}_{\Delta,B}$.

Proof. If $\alpha : t \overset{\sigma}{\leadsto}{}^*_{\Delta,B} t\sigma{\downarrow}_{\Delta,B}$ such that σ is Δ, B-normalized and there are no substitutions ρ, ρ' such that $t \overset{\rho}{\leadsto}{}^*_{\Delta,B} t\rho{\downarrow}_{\Delta,B}$, $t\sigma{\downarrow}_{\Delta,B} =_B (t\rho{\downarrow}_{\Delta,B})\rho'$, $\sigma|_{Var(t)} =_B (\rho\rho')|_{Var(t)}$, and $\rho' \neq id$, then it is sufficient to show that every narrowing step in α has a Δ, B-normalized substitution and that substitution is minimal w.r.t. $\leq$.

The first fact is obvious because if one narrowing step has a non-normalized substitution, composing more substitutions is not going to make the whole substitution normalized.

The second fact is proved by contradiction. Let us consider a narrowing step $i \in \{1, \ldots, n\}$ in α, i.e. $t_i \overset{\sigma_i}{\leadsto}_{\Delta,B} t_{i+1}$, such that σ_i is not minimal w.r.t. $\leq$. That is, there is an alternative narrowing step from t_i, i.e., $t_i \overset{\tau}{\leadsto}_{\Delta,B} w$ with a strictly more general substitution τ, i.e., there is a substitution τ' s.t. $\sigma_i|_{Var(t_i)} =_B (\tau\tau')|_{Var(t_i)}$ and $\tau' \neq id$. Moreover, we have to consider that there is no narrowing sequence $w \overset{\rho}{\leadsto}{}^*_{\Delta,B} t_n$ such that $\sigma|_{Var(t)} =_B (\sigma_1 \cdots \sigma_{i-1}\tau\rho)|_{Var(t)}$; otherwise the contradiction is pointless. Then, we have that $t_i\sigma_i \rightarrow_{\Delta,B} t_{i+1}$ and that there is a term w' such that $t_i\sigma_i \rightarrow_{\Delta,B} w'$ and $w' =_B w\tau'$ (indeed, using the very same rule and position used in the narrowing step $t_i \overset{\tau}{\leadsto}_{\Delta,B} w$). By confluence, there is a term s such that $t_{i+1} \rightarrow^*_{\Delta,B} s$ and $w' \rightarrow^*_{\Delta,B} s$. But then, for any narrowing sequence $s \overset{\rho}{\leadsto}{}^*_{\Delta,B} u$ such that $\rho|_{Var(t_{i+1})} =_B (\sigma_{i+1} \cdots \sigma_n)|_{Var(t_{i+1})}$, there is a narrowing sequence $t \overset{\nu}{\leadsto}{}^*_{\Delta,B} t\nu{\downarrow}_{\Delta,B}$ such that $\nu = (\sigma_1 \cdots \sigma_{i-1}\tau\rho')|_{Var(t)}$ for ρ' such that $\rho|_{Var(s)} =_B \rho'\tau'|_{Var(s)}$. Therefore, we have a contradiction because ν is strictly more general than σ. □

Note that the previous theorem is only valid when Δ is confluent modulo B, instead of just *ground confluent* [15] modulo B, as shown by the following example.

Example 5. Let us consider the following rewrite theory, which is terminating and ground confluent but not confluent:

$$f(x) = 0 \tag{8}$$
$$f(x) = g(x) \tag{9}$$
$$g(0) = 0 \tag{10}$$
$$g(s(x)) = g(x) \tag{11}$$

If we consider the term $f(x)$ and the narrowing step taking the first equation, then we compute the most general substitution. However, if we consider $f(x)$ and the narrowing step that takes the second equation, we will compute an infinite number of substitutions, and no one of the them is more general than the identity substitution, computed with the first equation.

Note that the relation $\rightsquigarrow^*_{\underline{\Delta},B}$ can still have many infinite narrowing derivations. However, if (Δ, B) has the finite variant property, those infinite derivations can be avoided.

Theorem 7 (Computing the Finite Variants II). *Let (Δ, B) be a finite variant decomposition of an order-sorted equational theory (Σ, E). Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\#_{\Delta,B}(t) = n$. Then $(s, \sigma) \in FV_{\Delta,B}(t)$ if and only if there is a narrowing derivation $t \overset{\sigma'}{\rightsquigarrow}{}^{\leq n}_{\underline{\Delta},B} s$ such that $\sigma \simeq_B \sigma'$, s is $\rightarrow_{\Delta,B}$-irreducible and σ is $\rightarrow_{\Delta,B}$-normalized.*

Proof. By Proposition 2 and Theorem 6. □

Even without assuming the finite variant property, another possibility is combining $\rightsquigarrow^*_{\underline{\Delta},B}$ with narrowing strategies that can avoid useless infinite narrowing derivations such as natural narrowing [7] or finite representations of an infinite search space [6]. This is left for future work.

4.2 Strongly right-irreducible equational theories

We study a special class of rewrite theories for which we can obtain useful results about variant narrowing. The following definition is well-known and generalizes the notion of irreducible term from rewriting to narrowing.

Definition 10 (strongly irreducible). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory. We say that a term t is strongly $\rightarrow_{\Delta,B}$-irreducible if for any $\rightarrow_{\Delta,B}$-normalized substitution σ, the term $t\sigma$ is $\rightarrow_{\Delta,B}$-irreducible.*

Strongly irreducibility can be easily checked by narrowing.

Lemma 4. *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties (1)–(6). Given a term t with variables, t is strongly irreducible if and only if there is no term s and substitution σ such that $t \overset{\sigma}{\rightsquigarrow}_{\Delta,B} s$.*

Proof. The *only if* part is immediate by contradiction, i.e., if there is a term s and a substitution σ such that $t \overset{\sigma}{\rightsquigarrow}_{\Delta,B} s$, then, by confluence modulo B, $t(\sigma{\downarrow_{\Delta,B}})$ is not $\rightarrow_{\Delta,B}$-irreducible. For the *if* part, also by contradiction, we just use Lemma 1, i.e., if t is not strongly irreducible, then there is a Δ, B-normalized substitution σ and a term s such that $t\sigma \rightarrow_{\Delta,B} s$ and, by Lemma 1, there is a substitution σ' and a term s' such that $t \overset{\sigma'}{\rightsquigarrow}{}^*_{\Delta,B} s'$. □

With this notion we can define a special type of rewrite theory which, under an extra condition shown below, satisfies the boundedness property.

Definition 11 (strongly right-irreducible TRS). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory. We say $\mathcal{R}$ is* strongly right-irreducible *if every right-hand side of Δ is strongly $\rightarrow_{\Delta,B}$-irreducible.*

We need an extra condition on the decomposition (Δ, B) to ensure the appropriate boundedness property.

Definition 12 (innermost preserving). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted*
rewrite theory satisfying properties (1)–(6) *that does not include* collapsing equations*, i.e., of the form $t = t|_p$. We say that the theory $\mathcal{R}$ is* innermost preserving *if for any symbol $f \in \Sigma$ and $\rightarrow_{\Delta,B}$-irreducible terms $t_1, ..., t_n$, either $f(t_1, \ldots, t_n)$ is $\rightarrow_{\Delta,B}$-irreducible or there is a $\rightarrow_{\Delta,B}$ step at the top position with a $\rightarrow_{\Delta,B}$-normalized substitution.*

Given a rewrite theory (Σ, B, Δ), we denote the set of *defined* symbols by $\mathcal{D} = \{root(l) \mid l \rightarrow r \in \Delta\}$ and the set of *constructor* symbols as $\mathcal{C} = \Sigma - \mathcal{D}$. Note that, for an order-sorted rewrite theory $\mathcal{R} = (\mathcal{D} \uplus \mathcal{C}, B, \Delta)$ satisfying properties (1)–(6), if Ω are the function symbols used in the equations B, and $\Omega \cap \mathcal{D} = \emptyset$, then $\mathcal{R}$ trivially satisfies the innermost preserving property. For the more general case, we can provide a general characterization similar to E-coherence.

Lemma 5. *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. $\mathcal{R}$ is innermost preserving if and only if $\forall t_1, t_2, t_3$ such that $t_1 \rightarrow_{\Delta,B} t_2$, $t_1 =_B t_3$, and t_3 is of the form $f(u_1, \ldots, u_n)$ for $f \in \Sigma$ with $u_1, \ldots, u_n \rightarrow_{\Delta,B}$-irreducible, $\exists t_4$ such that $t_3 \stackrel{\Lambda}{\rightarrow}_{\Delta,B} t_4$ using a $\rightarrow_{\Delta,B}$-normalized substitution.*

Proof. Immediate. □

Based on the above lemma, general procedures to check that $\mathcal{R}$ is innermost preserving can be defined similar to procedures to check E-coherence. However, this is left for future work. The following result links strongly irreducible and innermost preserving rewrite theories with the boundedness property.

Lemma 6. *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a strongly right-irreducible, innermost preserving, order-sorted rewrite theory. Then $\mathcal{R}$ has the boundedness property, where the bound $\#_{\Delta,B}(t)$ for a term t is the number of function symbols strictly above the $\rightarrow_{\Delta,B}$-irreducible subterms of t.*

Proof. Let us consider a term t and a $\rightarrow_{\Delta,B}$-normalized substitution σ. Note that, by definition of $\rightarrow_{\Delta,B}$, any redex of $t\sigma$ is located strictly above the $\rightarrow_{\Delta,B}$-irreducible subterms of $t\sigma$, i.e., in a position of t. We prove the result by induction on $\#_{\Delta,B}(t) = n$.

1. $(n = 0)$ In this case, t is a variable and $t\sigma$ is $\rightarrow_{\Delta,B}$-irreducible, or a constant that it is $\rightarrow_{\Delta,B}$-irreducible. In both cases, the conclusion follows.
2. $(n > 0)$ Since $\mathcal{R}$ is innermost preserving, if $t\sigma$ is not normalized, there is a position $p \in Pos_\Sigma(t\sigma)$, a rule $l \rightarrow r \in \Delta$, and a $\rightarrow_{\Delta,B}$-normalized substitution θ such that $t\sigma|_p =_B l\theta$ and $t\sigma|_p = f(u_1, \ldots, u_k)$ where $u_1, \ldots, u_k$ are $\rightarrow_{\Delta,B}$-irreducible. Note also that $p \in Pos_\Sigma(t)$, since σ is $\rightarrow_{\Delta,B}$-normalized. Since r is strongly $\rightarrow_{\Delta,B}$-irreducible and θ is $\rightarrow_{\Delta,B}$-normalized, $r\theta$ is $\rightarrow_{\Delta,B}$-irreducible. Then, let $t' = (t\sigma)[r\theta]_p$, $\#_{\Delta,B}(t') < \#_{\Delta,B}(t)$, at least in one unit, since any redex of t' is strictly above the $\rightarrow_{\Delta,B}$-irreducible subterms of t'. Thus, the conclusion follows by induction hypothesis. □

Example 6. Building on top of Example 1, let t_1 and t_2 be irreducible terms (w.r.t. $\rightarrow_{\Delta/B}$), then $t_1 \oplus t_2$ can be reduced to its normal form using at most one reduction step, as follows. Note that t_1 and t_2 are terms of the form $u_1 \oplus \cdots \oplus u_n$ and $v_1 \oplus \cdots \oplus v_m$ with $n, m \geq 1$. If all the terms $u_1, \ldots, u_n, v_1, \ldots, v_m$ are pairwise distinct and different from 0, $t_1 \oplus t_2$ is an irreducible term. If all the terms $u_1, \ldots, u_n, v_1, \ldots, v_m$ are pairwise distinct but there is one 0 among them, then rule (1) can be applied at the top position with a normalized substitution. Otherwise, for all $t_1 \oplus t_2$ having an even number of equal terms in $u_1, \ldots, u_n, v_1, \ldots, v_m$, the rule (3) can take all those elements at the same time in one unique application at the top position, computing a normalized substitution (splitting the evenly repeated terms into the two occurrences of variable X) and providing the normal form of $t_1 \oplus t_2$. Note that it is not possible to have an odd number of 0's and at least one duplicated term at the same time. The reason for that is that 0 can only appear by itself, since $0 \oplus X$ is not irreducible. On the other hand, a duplicated term appearing in t_1 (resp. t_2) means that t_1 (resp. t_2) is not irreducible either. Similarly, consider two irreducible terms t_1 and t_2, $pk(t_1, t_2)$ and $sk(t_1, t_2)$ can be reduced to their normal form in at most one reduction step, as follows. $pk(t_1, t_2)$ can only be rewritten whenever $t_2 = sk(t_1, t_3)$ for some new t_3 that is also irreducible, otherwise it is already in normal form. In case it is not in normal form one step of rewriting results in t_3 which is a normal form. Similarly for $sk(t_1, t_2)$.

Note that Δ has the boundedness property as it is a strongly right-irreducible rewrite theory and innermost preserving.

Furthermore, the innermost preserving property is essential, as shown in the following example.

Example 7. Consider again Example 1 but let us assume now that variable X in rules (2) and (3) are of a sort Element and cannot match a term rooted by $\oplus$. Let us consider the term $t = a \oplus (b \oplus (a \oplus b))$ where a, b are constants. Rule (2) cannot be applied at any position, and only rule (3) can be applied at the top. However, there is no possible application with a normalized substitution and thus term t cannot be reduced to its normal form in one step, i.e., $a \oplus (b \oplus (a \oplus b)) \rightarrow_{\Delta,B} b \oplus b \rightarrow_{\Delta,B} 0$. Indeed, note that given a term $s = x \oplus y$ and any normalized substitution σ, the number of reduction steps for $s\sigma$ to reach its normal form clearly depends on the number of $\oplus$ symbols introduced by σ.

Finally, the main result of our paper is the following.

Theorem 8 (Computing the Finite Variants III). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a strongly right-irreducible, innermost preserving, order-sorted rewrite theory. The bound on the number of narrowing steps, denoted $\#_{\Delta,B}(t)$, is the number of symbols strictly above the $\rightarrow_{\Delta,B}$-irreducible subterms of t. Let $t \in \mathcal{T}_\Sigma(\mathcal{X})$ and $\#_{\Delta,B}(t) = n$. Then $(s, \sigma) \in FV_{\Delta,B}(t)$ if and only if there is a narrowing derivation $t \overset{\sigma'}{\underset{\Delta,B}{\leadsto}}{}^{\leq n} s$ such that $\sigma \simeq_B \sigma'$, s is $\rightarrow_{\Delta,B}$-irreducible and σ is $\rightarrow_{\Delta,B}$-normalized.*

Proof. For the *if* part, the proof is immediate. That is, given $\#_{\Delta,B}(t) = n$, by definition, for each narrowing sequence $t \overset{\sigma}{\rightsquigarrow}{}^{\leq n}_{\underline{\Delta},B} s$ such that s is $\rightarrow_{\Delta,B}$-irreducible and σ is $\rightarrow_{\Delta,B}$-normalized, $(s,\sigma) \in FV_{\Delta,B}(t)$.

For the *only if* part, we prove by structural induction that the restricted depth of the narrowing tree is not a problem.

- If t is a variable, then t is its normal form.
- If t is a constant, then, by Lemma 6, the normal form of t is obtained in at most one reduction step.
- If $t = f(t_1, \ldots, t_k)$, then, by induction hypothesis, for each $1 \leq i \leq k$, t_i can be reduced to its normal form in $\#_{\Delta,B}(t_i)$ many steps or less, which is the number of symbols strictly above the $\rightarrow_{\Delta,B}$-irreducible subterms of t_i. Therefore, we can construct a rewriting sequence $f(t_1, \ldots, t_k) \rightarrow^m_{\Delta,B} f(t'_1, \ldots, t'_k)$ such that $t'_i = t_i{\downarrow_{\Delta,B}}$ and $m \leq \#_{\Delta,B}(t_1) + \cdots + \#_{\Delta,B}(t_k)$. Now, since $\mathcal{R}$ is innermost preserving and strongly right-irreducible, the normal form of $f(t'_1, \ldots, t'_k)$ is obtained in at most one reduction step. Therefore, the normal form of t has been obtained in less or equal number of steps than the number of symbols strictly above the $\rightarrow_{\Delta,B}$-irreducible subterms of t.

Note that although there can be other reduction sequences longer than that number of symbols in t, by confluence modulo B, those sequences yield the same normal form and thus are irrelevant. □

5 Variant Narrowing and Equational Unification

Variant narrowing provides a complete equational unification procedure.

Theorem 9 (Variant-narrowing unification procedure). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6)*. Let t, t' be two terms. Then, $\sigma \in CSU_{\Delta \uplus B}(t = t')$ if and only if $(t \approx t') \overset{\sigma}{\rightsquigarrow}{}^*_{\underline{\widehat{\Delta}},B} \mathtt{tt}$, recall the definition of $\widehat{\Delta}$ in the footnote of Theorem 4.*

Proof. By Theorem 7 and Theorem 4. Note that the rewrite theory $\widehat{\mathcal{R}} = (\widehat{\Sigma}, B, \widehat{\Delta})$ satisfies properties (1)–(6), since, symbols $\approx$ and $\mathtt{tt}$ in $\widehat{\Sigma}$ and the rule $x \approx x \rightarrow \mathtt{tt}$ in $\widehat{\Delta}$ do not interfere with properties (1)–(6), for instance, with B-coherence. □

In the case that a rewrite theory has the boundedness property, then we can compute a bound on the number of narrowing steps needed to compute a complete set of unifiers.

Corollary 1 (Bounded variant-narrowing unification procedure). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *that also has the boundedness property. Let t, t' be two terms. Then the set $CSU_{\Delta \uplus B}(t = t')$ of unifiers is* finitary*, and we can put a bound on the number of narrowing steps $\rightsquigarrow^*_{\underline{\Delta},B}$ from the term $t \approx t'$ needed to compute $CSU_{\Delta \uplus B}(t = t')$. The bound $\#_{\Delta,B}(t \approx t') = \#_{\Delta,B}(t) + \#_{\Delta,B}(t') + 1$.*

The procedure of Corollary 1 for equational unification is unsatisfactory in practice, because a bigger bound allows more useless narrowing sequences up to such bound. Thus, for a finite variant decomposition (Δ, B) of an equational theory E, the unification problem $CSU_{\Delta \uplus B}(t = t')$ is implicitly solved in [1] using the variants.

Theorem 10 (Finite Variant unification procedure). *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be an order-sorted rewrite theory satisfying properties* (1)–(6) *that has also the boundedness property. To obtain the complete set of $\Delta \uplus B$-unifiers of two terms t and t' we*

1. *compute their E-variants, say $FV_{\Delta \uplus B}(t) = \{(t_1, \sigma_1), \ldots, (t_n, \sigma_n)\}$ and $FV_{\Delta \uplus B}(t') = \{(t'_1, \sigma'_1), \ldots, (t'_m, \sigma'_m)\}$, and then*
2. *try B-unification on each pair t_i, t'_j for all $1 \leq i \leq n$ and $1 \leq j \leq m$.*

Then, $\theta \in CSU_{\Delta \uplus B}(t = t')$ if and only if there are $1 \leq i \leq n$, $1 \leq j \leq m$ and two substitutions ρ, ρ' such that $\rho \in (\sigma_i \cap_B \sigma'_j)$, $\rho' \in CSU_B(t_i = t'_j)$, and $\theta =_B \rho\rho'$; where the meet $\sigma \cap_B \sigma'$ of two substitutions σ, σ' is the set of most general substitutions τ such that there are minimal ρ and ρ' such that $\sigma\rho =_B \sigma'\rho'$, and $\tau = \sigma\rho$. Also the set of unifiers created this way forms a complete set of unifiers. The set of unifiers is a minimal set of unifiers, if the unification procedure for B is also minimal.

Proof. We first show that all unifiers are actually covered by this procedure. For all unifiers of t and t', i.e. $\forall \sigma \in CSU_{\Delta \uplus B}(t = t')$ we have that there are $(w, \sigma_1) \in FV_{\Delta \uplus B}(t)$, $(w', \sigma_2) \in FV_{\Delta \uplus B}(t')$, and substitutions θ, θ' such that $t\sigma{\downarrow_{\Delta,B}} =_B w\theta$ and $t'\sigma{\downarrow_{\Delta,B}} =_B w'\theta'$. By definition, $t\sigma =_{\Delta,B} t'\sigma$, i.e., $t\sigma{\downarrow_{\Delta,B}} =_B t'\sigma{\downarrow_{\Delta,B}}$ which implies $w\theta =_B t\sigma{\downarrow_{\Delta,B}} =_B t'\sigma{\downarrow_{\Delta,B}} =_B w'\theta'$.

Then we show that all θ created this way are $\Delta \uplus B$-unifiers. Assume θ was created from unifying (t_i, σ_i) and (t'_j, σ'_j), then $t\sigma_i =_{\Delta,B} t_i$, $t'\sigma'_j =_{\Delta,B} t'_j$, and $t_i\sigma =_B t'_j\sigma$, so $t\sigma_i\sigma =_{\Delta,B} t'\sigma'_j\sigma$ and as σ_i and σ'_j are compatible we have $t\sigma_i\sigma\sigma'_j =_{\Delta,B} t'\sigma'_j\sigma\sigma_i$, i.e., with $\theta = \sigma_i\sigma'_j\sigma$ we have $t\theta =_{\Delta,B} t'\theta$ which means θ is indeed a $\Delta \uplus B$-unifier.

As the procedure used for the B-unification returns minimal sets of unifiers for each pair of variants (t_i, σ_i) and (t'_j, σ'_j) the overall set of unifiers for t and t' generated this way is also minimal. That is because removing any one unifier from that set results in a set of unifiers that is not complete anymore, as the removed unifier is not covered by the remaining unifiers in the set, which is immediate by way of the definition of variants. □

Note that thanks to Proposition 1 we can filter out non-normalized substitutions and substitutions that have an alternative, more general one. This provides a complete and minimal set of substitutions. Indeed, by using the variant narrowing to compute $FV_{\Delta \uplus B}(t)$ we already filter out many unnecessary unifiers.

Example 8. Using the theory given in Example 1 with $E = \Delta \uplus B$ and the E-variants found in Example 2 we have for $t = M \oplus sk(K, pk(K, M))$ the set consisting of only one element, $(0, id)$, is a complete set of E-variants. For $t' = 0$

we have $(0, id)$ is a complete set of E-variants. Then we can answer the E-unification question for $t =_{\Delta \uplus B} t'$ by considering $0 =_B 0$ which has a positive answer with substitution id. Therefore we have that $id\,id\,id = id$ is an E-unifier of t and t'.
For the term $s = X \oplus sk(K, pk(K, Y))$ we have $(0, X/Y)$ and $(X \oplus Y, id)$ as E-variants. Considering $s' = a \oplus b$ with a, b constants we have that $(a \oplus b, id)$ is a complete set of E-variants for s'. Then the E-unification question of $s =_E s'$ can be answered by considering the combination of E-variants. First, $0 =_B a \oplus b$ has no solution while $X \oplus Y =_B a \oplus b$ has two solutions, $\{X/a, Y/b\}$ and $\{X/b, Y/a\}$ which both are solutions of the original problem $s =_E s'$, since id was the substitution part of all E-variants.

5.1 Special case of strongly right-irreducible theories

Corollary 2. *Let $\mathcal{R} = (\Sigma, B, \Delta)$ be a strongly right-irreducible, innermost preserving, order-sorted rewrite theory. Let $t, t' \in \mathcal{T}_\Sigma(\mathcal{X})$. The set $CSU_{\Delta \uplus B}(t = t')$ of unifiers of t and t' is finitary and complete and is computed by the procedure of Theorem 10, where the variants are computed by the procedure of Theorem 8.*

Example 9. Using the theory given in Example 1, the unification question for two terms t and t' can be answered by going to depth $\#_\oplus(t) + \#_{sk}(t) + \#_{pk}(t)$ (where $\#_\oplus(t)$ denotes the number of occurrences of $\oplus$ in t, likewise for $\#_{pk}(t)$ and $\#_{sk}(t)$) in the narrowing tree for t, going to depth $\#_\oplus(t') + \#_{sk}(t') + \#_{pk}(t')$ in the narrowing tree for t', and then using AC-unification on the variants of t and t', i.e. all the normalized terms in the tree.

Example 10. Using the results from Example 2 to solve the E-unification problem $t =_E t'$ with $t = M \oplus sk(K, pk(K, M))$ and $t' = 0$. We know that $\{(0, id)\}$ is a complete set of E-variants for t. Obviously, $\{(t', id)\}$ is a complete set of E-variants for t'. Of course $0 =_B t'$ can be answered positively and therefore $t =_E t'$ has a positive answer and the identity substitution id is a complete set of E-unifiers.

Similarly for the E-unification $s =_E r$ with $s = X \oplus sk(K, pk(K, Y))$ and $r = 0$, we have $s' = 0$, $s'' = X \oplus Y$ and $S = \{(s', \theta'), (s'', id)\}$, with θ' such that $\theta' = \{X/Y\}$, is a complete set of E-variants of s. For $r = 0$ we again have $\{(r', id)\}$ with $r' = 0$ a complete set of E-variants. Also, the answer to the unification problem is again positive, with $\theta = \{X/Y\}$, and then θ is the complete set of E-unifiers because $s' = 0 =_B 0 = r'$ with the id substitution in the last step, the id substitution for r' and θ as the substitution required for s'.

Let us illustrate with an example that indeed our optimizations do not just improve efficiency of the computation of unifiers, but that without those optimizations we get unnecessarily large sets of complete unifiers.

Example 11. Using the running example, Example 1, and using $\rightsquigarrow^*_{\Delta, B}$ instead of $\rightsquigarrow^*_{\underline{\Delta}, B}$, which should be used according to Theorem 8, we get the following variants for the term $t = M \oplus sk(K, pk(K, M))$. Of course $t \overset{id}{\rightsquigarrow}_{\Delta, B} 0$, thus $(0, id)$

is a variant, but also $t \overset{M/0}{\leadsto}_{\Delta,B} 0$, so $(0, M/0)$ is a variant. Then solving $t =_E 0$ as done in Example 10 we have $(0, id)$ a variant for 0 and we thus get two unifiers, id and $M/0$ where $M/0$ is obviously subsumed by id and should be omitted.

6 Related Work and Conclusions

Unification modulo an equational theory E has already been studied in the literature. The use of the basic narrowing strategy of [8] for unification modulo an the equational theory (Σ, E) that can be decomposed into $(\emptyset, \Delta)$ is the earliest work. Although it might seem that the basic narrowing strategy is subsumed into our variant strategy, this is not the case. Intuitively, variant narrowing and basic narrowing are both restrictions of ordinary narrowing that avoid sequences with non-normalized substitutions. Basic narrowing avoids any narrowing step performed within the computed substitutions whereas variant narrowing filters them when found.

Example 12. Consider the rewrite theory $(\Sigma, \emptyset, \Delta)$, the set of rules $\Delta = \{f(x) \to x, f(f(x)) \to x\}$, and the term $t = f(x)$. Basic narrowing performs only the following two narrowing steps $f(x) \overset{id}{\leadsto}_{\Delta} x$ and $f(x) \overset{\sigma}{\leadsto}_{\Delta} f(x')$ with $\sigma = \{x/f(x')\}$. Then, it stops, since the expression $f(x')$ was introduced by a substitution. This cuts any possible non-normalized substitution that could be generated by further instantiation of σ. Variant narrowing will perform only the first narrowing step, since the second contains a non-normalized substitution.

However, since the variant narrowing strategy does not carry any history of computed terms or substitutions, it is not able to avoid some useless narrowing sequences, whereas basic narrowing will avoid any of those sequences from the very beginning by avoiding narrowing inside the substitutions.

Example 13. Now, consider the previous rewrite theory $(\Sigma, \emptyset, \Delta)$ but with only the second rule, i.e., $\Delta = \{f(f(x)) \to x\}$. Basic narrowing performs only $f(x) \overset{\sigma}{\leadsto}_{\Delta} f(x')$ with $\sigma = \{x/f(x')\}$ and it stops. However, our variant narrowing will perform the following (infinite) narrowing sequence $f(x) \overset{\theta_1}{\leadsto}_{\Delta} f(x_1) \overset{\theta_2}{\leadsto}_{\Delta} f(x_2) \cdots$ with $\theta_1 = \{x/f(x_1)\}$, $\theta_{i+1} = \{x_i/f(x_{i+1})\}$, since every of the individual unifiers is normalized.

However, our argument (as well as others [1,16]) is that basic narrowing is too restrictive and indeed it can fail to be sound and complete when $B \neq \emptyset$, whereas variant narrowing is complete modulo axioms.

Example 14. Consider the following rewrite theory (Σ, B, Δ) from [1] where B contains associativity and commutativity of the operator $\times$ and $\Delta = \{a \times a \to 0, b \times b \to 0, a \times a \times Z \to Z, b \times b \times Z \to Z, 0 \times Z \to Z\}$. Given the term $X \times Y$, AC-basic narrowing is not able to provide the narrowing sequence $X \times Y \overset{\sigma}{\leadsto}_{\Delta,B} X' \times Y' \overset{\sigma'}{\leadsto}_{\Delta,B} 0$ with $\sigma = \{X/a \times X', Y/a \times Y'\}$ and $\sigma' = \{X'/b, Y'/b\}$, since the

term $X' \times Y'$ comes from the application of the unifier σ to the right-hand side Z of the rule $a \times a \times Z \to Z$. However, our variant narrowing is able to provide this narrowing sequence, since no non-normalized substitution is generated at any step.

In any case, there is an interesting result relating basic narrowing and the finite variant property: for strongly right-irreducible, innermost preserving, order-sorted rewrite theories $(\Sigma, \emptyset, \Delta)$, Lemma 6 shows that basic narrowing always terminates within the bound $\#_{\Delta,\emptyset}$.

Another related work is the repaired basic AC-narrowing strategy of [16], which considers implicit extensions instead of explicit extensions to overcome incompleteness. However, [16] considers only associativity and commutativity whereas we scale our results to more general axioms.

6.1 Conclusions

We have proposed variant narrowing as a narrowing modulo B procedure that achieves efficiency, in terms of having a potentially much smaller search space than full narrowing, without losing completeness. We have also shown how, when a theory E has the finite variant property, variant narrowing specializes to algorithms for both computing the finite variant and for computing a complete and minimal set of E-unifiers. Finally, we have given sufficient conditions on an equational theory E guaranteeing the finite variant property and giving an algorithm to compute the corresponding bound for each term.

Much work remains ahead. Other classes of equational theories E enjoying the finite variant property, and general algorithms for computing the corresponding bound for such theories should be studied. Algorithms automating the checking of the innermost preserving property should also be developed. We are also working on, and plan to finish soon, an implementation of variant narrowing that will provide both a prototype to experiment with variant narrowing and insights on how to further optimize this kind of narrowing. We specifically plan to use this prototype as a component of the Maude-NPA tool to experiment with it in the context of formal analyses of cryptographic protocols modulo cryptographic theories. Finally, modularity results, allowing us to know when modular combinations of theories enjoying the finite variant property also enjoy the same property is a topic worth investigating, since it will support modular combinations of the corresponding unification algorithms.

Acknowledgments. We would like to thank Hubert Comon and Stephanie Delaune for useful discussion on the finite variant problem. We would also like to thank Stephanie Delaune, Claude Kirchner and Hélène Kirchner for useful discussion on narrowing modulo.

This research has been partially supported by ONR Grant N00014-02-1-0715 and NSF Grant CNS-07-16638. S. Escobar has been partially supported by the EU (FEDER) and the Spanish MEC, under grants TIN2004-7943-C04-01 and TIN2007-68093-C02-02, Integrated Action HA 2006-0007, and Generalitat Valenciana GV06/285.

References

1. H. Comon-Lundh and S. Delaune. The finite variant property: How to get rid of some algebraic properties. In J. Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 294–307. Springer, 2005.
2. N. Dershowitz, S. Mitra, and G. Sivakumar. Decidable matching for convergent systems (preliminary version). In D. Kapur, editor, *CADE*, volume 607 of *Lecture Notes in Computer Science*, pages 589–602. Springer, 1992.
3. S. Escobar, J. Hendrix, , C. Meadows, and J. Meseguer. Diffie-hellman cryptographic reasoning in the Maude-NRL Protocol Analyzer. In *Proc. of the Second International Workshop on Security and Rewriting Techniques (SecReT 2007)*, 2007.
4. S. Escobar, C. Meadows, and J. Meseguer. A rewriting-based inference system for the nrl protocol analyzer and its meta-logical properties. *Theor. Comput. Sci.*, 367(1-2):162–202, 2006.
5. S. Escobar, C. Meadows, and J. Meseguer. Equational cryptographic reasoning in the maude-nrl protocol analyzer. *Electronic Notes in Theoretical Computer Science*, 171(4):23–36, 2007.
6. S. Escobar and J. Meseguer. Symbolic model checking of infinite-state systems using narrowing. In F. Baader, editor, *RTA*, volume 4533 of *Lecture Notes in Computer Science*, pages 153–168. Springer, 2007.
7. S. Escobar, J. Meseguer, and P. Thati. Natural narrowing for general term rewriting systems. In J. Giesl, editor, *Term Rewriting and Applications, 16th International Conference, RTA 2005, Nara, Japan, April 19-21, 2005, Proceedings*, volume 3467 of *Lecture Notes in Computer Science*, pages 279–293. Springer, 2005.
8. J.-M. Hullot. Canonical forms and unification. In W. Bibel and R. A. Kowalski, editors, *CADE*, volume 87 of *Lecture Notes in Computer Science*, pages 318–334. Springer, 1980.
9. J.-P. Jouannaud, C. Kirchner, and H. Kirchner. Incremental construction of unification algorithms in equational theories. In J. Díaz, editor, *ICALP*, volume 154 of *Lecture Notes in Computer Science*, pages 361–373. Springer, 1983.
10. D. Kapur and P. Narendran. Matching, Unification and Complexity. *ACM SIGSAM Bulletin*, 21(4):6–9, 1987.
11. J. Meseguer. Conditioned rewriting logic as a united model of concurrency. *Theor. Comput. Sci.*, 96(1):73–155, 1992.
12. J. Meseguer. Membership algebra as a logical framework for equational specification. In F. Parisi-Presicce, editor, *WADT*, volume 1376 of *Lecture Notes in Computer Science*, pages 18–61. Springer, 1997.
13. J. Meseguer and P. Thati. Symbolic reachability analysis using narrowing and its application to verification of cryptographic protocols. *Higher-Order and Symbolic Computation*, 20(1-2):123–160, 2007.
14. S. Mitra. *Semantic Unification for Convergent Rewrite Systems*. PhD thesis, University Illinois at Urbana-Champaign, 1994.
15. TeReSe, editor. *Term Rewriting Systems*. Cambridge University Press, Cambridge, 2003.
16. E. Viola. E-unifiability via narrowing. In A. Restivo, S. R. D. Rocca, and L. Roversi, editors, *ICTCS*, volume 2202 of *Lecture Notes in Computer Science*, pages 426–438. Springer, 2001.

17. P. Viry. Equational rules for rewriting logic. *Theor. Comput. Sci.*, 285(2):487–517, 2002.